Technical Report 13-004

Developing an Effective Plan for Smart Sanctions: A Network Analysis Approach

Marc Anthony Johnson, Lauren Kewley, and Daniel Evans

U.S. Military Academy, West Point NY

October 2012

United States Military Academy
Network Science Center

Approved for public release; distribution is unlimited.

U.S. Military Academy
Network Science Center

Authorized and approved for distribution:

BG (R) CHRIS ARNEY, Ph.D.
Network Science Chair

COL JOHN M GRAHAM, Ph.D.
Director, Network Science Center

Technical review by

MAJ Paulo Shakarian, Ph.D., Department of Electrical Engineering and Computer Science, U.S. Military Academy

CPT(P) Jarrod Shingleton, Department of Mathematical Sciences, U.S. Military Academy

NOTICES

DISTRIBUTION: Primary distribution of this Technical Report has been made by the U.S. Military Academy Network Science Center. Please address correspondence concerning distribution of reports to: Network Science Center, U.S. Military Academy, 646 Swift Road, West Point, NY 10996

FINAL DISPOSITION: This Technical Report may be destroyed when it is no longer needed. Please do not return it to the U.S. Military Academy Network Science Center.

NOTE: The findings in this Technical Report are not to be construed as an official Department of the Army position, unless so designated by other authorized documents

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* 31-10-2012	**2. REPORT TYPE** Technical Report	**3. DATES COVERED** *(From - To)* June 2012-Sept 2012
4. TITLE AND SUBTITLE **Developing an Effective Plan for Smart Sanctions: A Network Analysis Approach**		**5a. CONTRACT NUMBER** n/a **5b. GRANT NUMBER** n/a **5c. PROGRAM ELEMENT NUMBER** n/a
6. AUTHOR(S) **Marc Anthony Johnson, Lauren Kewley, and Daniel Evans**		**5d. PROJECT NUMBER** ARO NetSci 03 **5e. TASK NUMBER** n/a **5f. WORK UNIT NUMBER** n/a
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Network Science Center, U.S. Military Academy 601 Cullum Road, Thayer Hall Room 119 West Point, NY 10996		**8. PERFORMING ORGANIZATION REPORT NUMBER** n/a
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) U.S.Army Research Office Triangle Park, NC		**10. SPONSOR/MONITOR'S ACRONYM(S)** USMA NSC **11. SPONSOR/MONITOR'S REPORT NUMBER(S) 13-004**

12. DISTRIBUTION / AVAILABILITY STATEMENT

Unlimited Distribution

13. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the authors and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

14. ABSTRACT

In this project, we apply develop a set of data and a network model that realistically simulates the Iranian nuclear development program. We then utilize several network analysis techniques including Node Classification, Centrality Distribution, and a Score boarding technique in order to evaluate this data set. These techniques are potentially a quantitative method to better evaluate the effectiveness of existing or, additional imposition of, sanctions in order to hinder the progress of Iran's nuclear program.

15. SUBJECT TERMS

Network Science, Algorithms, Iran, Sanctions, Social Network

16. SECURITY CLASSIFICATION OF: a. REPORT	b. ABSTRACT	c. THIS PAGE	**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL	20	Tish Torgerson **19b. TELEPHONE NUMBER** *(include area code)* 845-938-0804

Technical Report 13-004

Developing an Effective Plan for Smart Sanctions: A Network Analysis Approach

Marc Anthony Johnson, Lauren Kewley, and Daniel Evans

U.S. Military Academy, West Point NY

U.S. Military Academy Network Science Center
601 Cullum Road, Thayer Hall Room 119, West Point, NY 10996

31 October 2012

Approved for public release; distribution is unlimited.

ACKNOWLEDGEMENT

This work was supported by the U.S. Army Research Organization, Project No. 1JO1XR059 and 2EDATXR021.

Daniel Evans supports this project through the Army Research Office's Scientific Support Program. Battelle Memorial Institute administers the Scientific Support Program for the Army Research Office.

October 2012

Developing an Effective Plan for Smart Sanctions: A Network Analysis Approach

Marc Anthony Johnson, Lauren Kewley, and Daniel Evans

Abstract

Social network analysis is a field of study that analyzes large amounts of data in order to determine interactions between entities in a network. Increasingly, organizations have gathered databases of information that they sort and analyze through the use of statistical methods. Alternatively, using network analysis can help identify prominent and influential actors and organizations in the data. This paper highlights strengths of network analysis in data parsing. The insights found through statistical network analysis gives decision makers an edge in effectiveness for making strategic decisions. This paper focuses on ways to use network measures to assist in the evaluation of the effectiveness of sanctions in Iran.

Introduction

Sanctions were first levied against Iran by the US in 1979 after Iran's 1979 Islamic revolution [1]. These sanctions were generally overlapping with measures taken by the United Nations (UN) and by European and Asian nations. However, some US sanctions, like the 1996 Iran Sanctions Act (ISA), "caused differences of opinion between the United States and its European allies because it mandates US imposition of sanctions against foreign firms"[2]. The objective of the sanctions has been to limit terrorism efforts in Iran as well as dissuade them from continuing their efforts at a nuclear weapon program. London's International Institute for Strategic Studies (IISS) reported that "sanctions imposed against Iran have thwarted Tehran's efforts to develop and produce long-range ballistic missiles capable of striking potential targets in Western Europe and beyond" [3]. However, some contend that sanctions will backfire by damaging the Iranian economy, thereby coercing a reliance on black market activity. This economic cascade ultimately consolidates power into the hands of the Islamic Revolutionary Guard Corps (IRGC), a special military force with strong ties to Ali Khamenei, by giving them an increasing stake in the Iranian economy.

We utilized a small sample of an Iranian data set in order to investigate some of the network analysis analytical methodologies available to researchers. Data collected in this paper is primarily a list of companies, organizations and people who have been targeted by sanctions imposed by the UN, US, or EU. The list was collected from open source information found on the Iran Watch (iranwatch.org) watchdog website. Using this data, which at first glance seems obtuse and unwieldy, we constructed network models in order to better understand the data.

Methodology

The selected entities found in the data were sanctioned because of their probable involvement in Iranian nuclear development programs. Interestingly, this made the network a snapshot of the nuclear program connections in Iran based on affiliations. Using open source internet accessible information we created a network of connections among Iranian organizations and individuals of interest to sanctioning committees in the United Nations (UN), European Union (EU) and the United States (US).

The data was obtained via a methodical analysis of the social and economic structures in Iran's political network. After an investigation of the macro environment in Iran, the team identified areas of the Iranian government and economy essential to understanding the climate in Iran. The team began investigating the Iranian Revolutionary Guard Corps (IRGC)-the primary organization responsible for the Iranian nuclear development program. The team then increased the network by widening concentrically to include *bonyads* and their structure within the political/economic/social environment. *Bonyads* are parastatal foundations that play a significant role in Iran's non-petroleum economy [4]. *Bonyads* themselves are inherently connected to many companies and fronts in Iran that have been sanctioned and identified by Iran Watch [5]. The entire Iran Watch list of sanctioned organizations was explored and actors chosen for inclusion in the network. Individuals and organizations with a direct relationship with the sanctioned companies were then also added to the network.

The entities were considered linked if they were a subsidiary of, employee/employer of, client of, or provided material support to another entity. This connection list effectively created an incidence matrix of connections that can be represented graphically and can also be used to generate an adjacency matrix. The constructed adjacency matrix was then analyzed to identify influential individuals and organizations. The team then explored different methods of network analysis to analyze the collected data.

Displayed in Table 1 is an example of the type of data collected and analyzed. The connections between entities were determined by any entity affiliated with another in the same row. A full table was created, allowing creation and manipulation of the adjacency matrix.

Entity	Type	Organization
7th of TirIndustrial Complex	Organization	LIMMT Economic and Trade Company
A. Askarzadeh	Individual	Irinvestship Ltd.
A. Azizi	Individual	Melli Bank PLC
A. Behzadi	Individual	Qualitest FZE
A. Johnson	Individual	IRGC-Air Force Al-Ghadir Missile Command
A.Q. Khan	Individual	Azar Ab Industries
A.R. Semnanipour	Individual	IRISL Europe GmbH
A. Sedghi	Individual	Melli Bank PLC
A. Zand	Individual	Melli Bank PLC
Abbas Fatemi Torshizi	Individual	Future Bank B.S.C.
Abbas Jalil Khamaneh	Individual	Iran o Misr Shipping Company
Abdolkarim Ghavami Far	Individual	Bank Mellat
Abdolnaser Hemmati	Individual	Bank Sina
Abdolreza Abed	Individual	Khatam ol Anbia
Abdul Aziz Ahmad Abdul Malek	Individual	Future Bank B.S.C.
Abdul Reza Shahlai	Individual	
Abzar Boresh Kaveh Company	Organization	Iran Khodro Company
Ade lAl-Mannai	Individual	Future Bank B.S.C.
Adel Ghobadizadeh	Individual	Post Bank
Adrian Baldacchino	Individual	IRGC Air Force
Aerospace Industries Organization	Organization	Ministry of Defense&Armed Forces Logistics
Afshin Roghani	Individual	Bank of Industry&Mine

Table 1: Example of collected data.

Network Manipulation

The adjacency matrix catalogs the connections between the different entities in collected data. Figure 1 shows a network graph of the connections. This does not seem helpful compared to the data presented in Table 1. It is a multi-mode network that is difficult to analyze with any level of confidence. However, matrix algebra can be used to create single mode networks for more effective analysis.

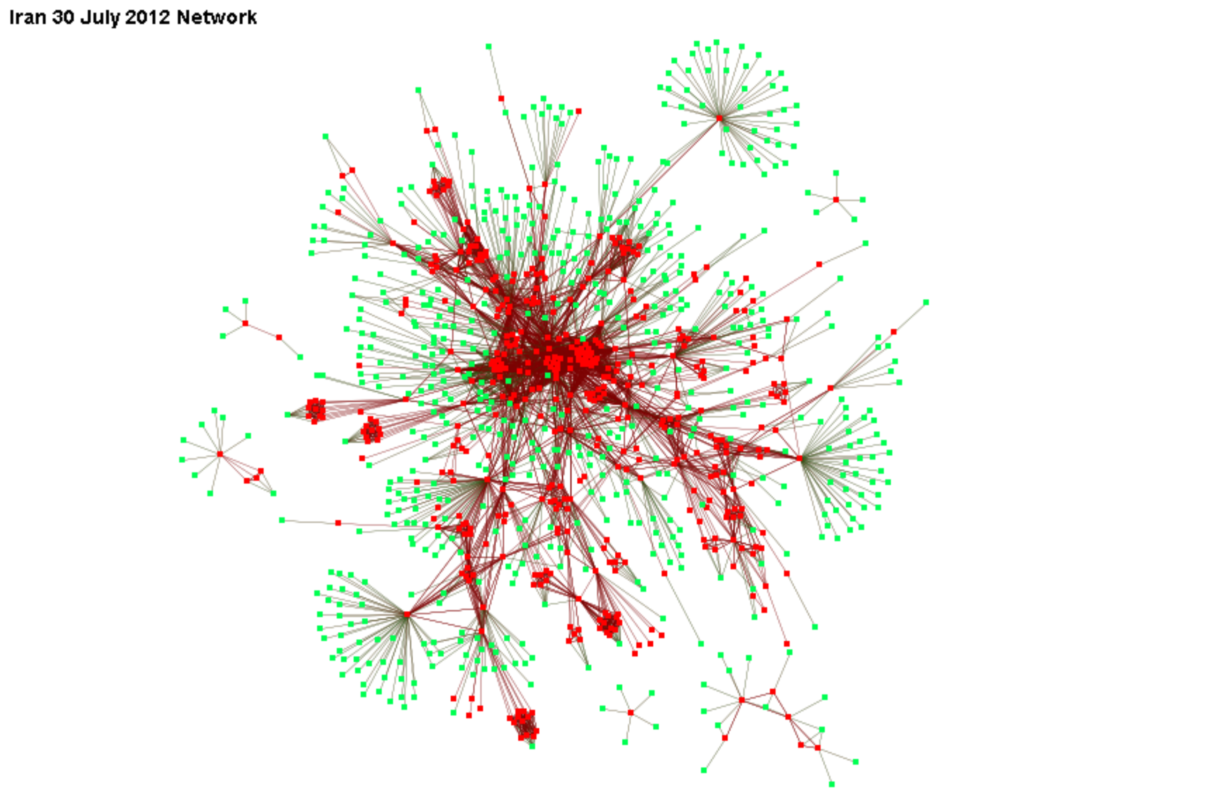


Figure 1: Meta Network of the Iran data. Organizations are colored green and entities of interest are colored red.

After multiplying the adjacency matrix by its transpose, a bi-partite network is created. It catalogs the agents connected to other agents through shared organizations or affiliates. This type of network can be analyzed much more effectively.

Once this network model is created, nodes were evaluated using several measures of centrality. The team then analyzed this network utilizing four of the most common measures; these measures will be described in more detail in the following section.

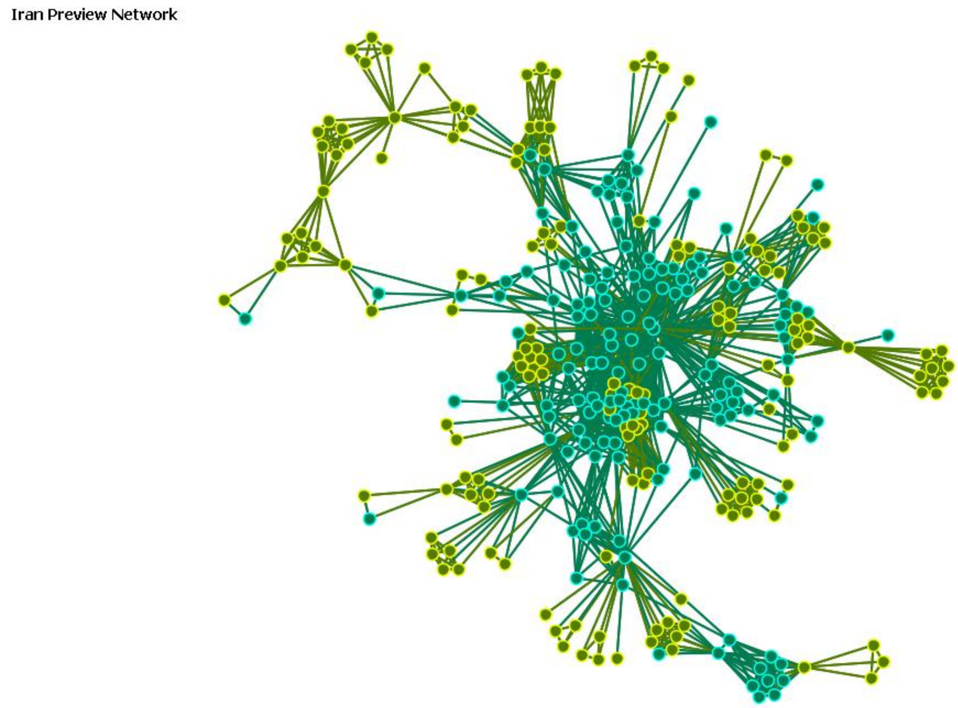


Figure 2: Iran Entities Network. Entities are colored by their type. The blue nodes are organizations, the green nodes are people.

powered by ORA, CASOS Center @ CMU

Centrality Measures

The four measures of focus in this paper are degree, betweenness, closeness, and eigenvector centrality.

Degree is defined as the number of edges incident upon a node. Let G = (V, E) be any undirected graph with *n* vertices and *m* edges. The degree $C_D v$ is defined as:

$$C_D v = \deg(v)$$

(Brandes and Erlebach, 2005) [6].

Betweenness is a centrality measure used often for longitudinal data. Let $\delta_{st}(v)$ denote the fraction of shortest paths between *s* and *t* that contain vertex v:

$$\delta_{st}(v) = \frac{\sigma_{st}(v)}{\sigma_{st}}$$

Where σ_{st} denotes the number of all shortest path between *s* and *t*. The betweenness centrality $C_B(v)$ of a vertex v is given by:

$$C_B(v) = \sum_{s \neq v \in V} \sum_{t \neq v \in V} \delta_{st}$$

(Brandes and Erlebach, 2005) [7].

Closeness is another centrality measure used to measure the geodesic distance of nodes to each other. If a node is shallow to other vertices, it tends to have short geodesic distances to other nodes in the graph. Closeness is the mean geodesic distance of a node from all other nodes reachable within the network. This is calculated with:

$$C_C(v) = \frac{1}{\sum_{t \in V/_v} d_G(v,t)}$$

The closeness($C_C(v)$) of a node is the reciprocal of the sum of all geodesic distances to all other vertices of *V* (Sabidussi, G., 1966) [8].

Eigenvector centrality is a measure of the importance of a node in the network. Let x_i denote the score of the *i*th node, and A_{ij} be the adjacency matrix of the network. Hence, A_{ij}=1 if the *i*th node is adjacent to the *j*th node, and A_{ij}=0 otherwise. More generally, the values in *A* can be real numbers representing the connection strengths like in a stochastic matrix. For the *i*th node, let the centrality score be proportional to the sum of the scores of all nodes which are connected to it, hence:

$$x_i = \frac{1}{\lambda} \sum_{j \in M(i)} x_j = \frac{1}{\lambda} \sum_{j=1}^{N} A_{i,j} x_j$$

Where, *M*(*i*) is the set of nodes that are connected to the *i*th node, *N* is the total number of nodes and λ is a constant. In vector notation this can be written as:

$$\lambda\mathbf{x} = A\mathbf{x}$$

(M. E. J. Newman, 2008) [9].

In simple terms, eigenvector centrality is a measure of how connected an actor is in the network. A high eigenvector centrality value means that an actor knows other nodes that have a high degree, or are very connected in the network. Likewise betweenness is a measure of how much of a go-between a node is in the network. Nodes with high betweenness values can be classified as gatekeepers in the network.

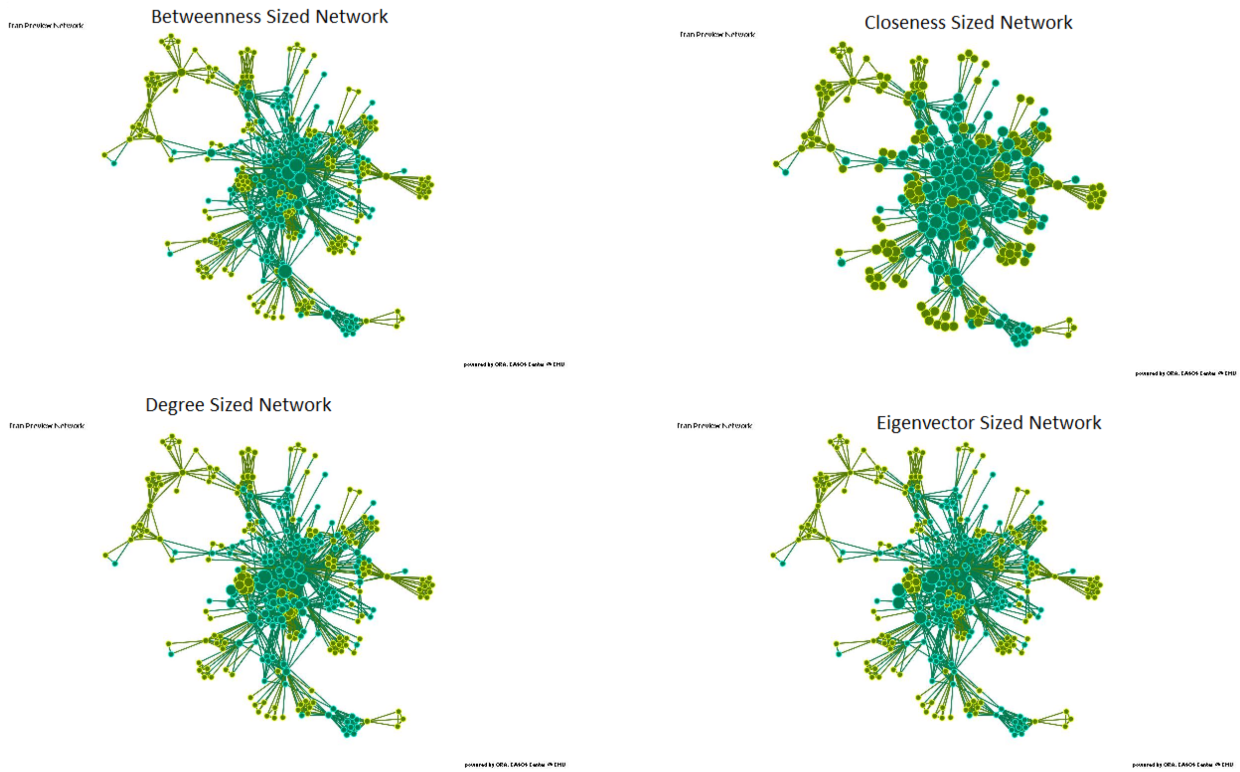


Figure 3: Entity Network with nodes sized according to the named measure. Larger images are in Appendix A-D.

The visualizations above illustrate the most influential nodes utilizing the four measures of centrality described above. The nodes are sized according to their different centrality values.

Descriptive Metric Analysis

Utilizing the centrality measures described previously, the data was analyzed to identify the most central nodes. Table 2 lists the four centralities and the top five nodes in each measure.

Rank	Betweenness centrality	Closeness centrality	Eigenvector centrality	Total degree centrality
1	Melli Bank PLC	Bank Mellat	Iran Electronics Industries	Iran Electronics Industries
2	Bank Tejarat	Noor Afza Gostar	Ahmad Rahzad	Aerospace Industries Organization
3	Europaeische-Iranische Handelsbank AG	Royal-Med Shipping Agency Ltd.	Ali Akbar Yahya	Bank Tejarat
4	Defense Industries Organization	Pearl Energy Company Ltd	F.N. Yaghmaei	Europaeische-Iranische Handelsbank AG
5	Asia Marine Network Pte. Ltd.	Shakhes Behbood Sanaat Company	Bahman Ghandi	Defense Industries Organization

Table 2: Rankings of top nodes.

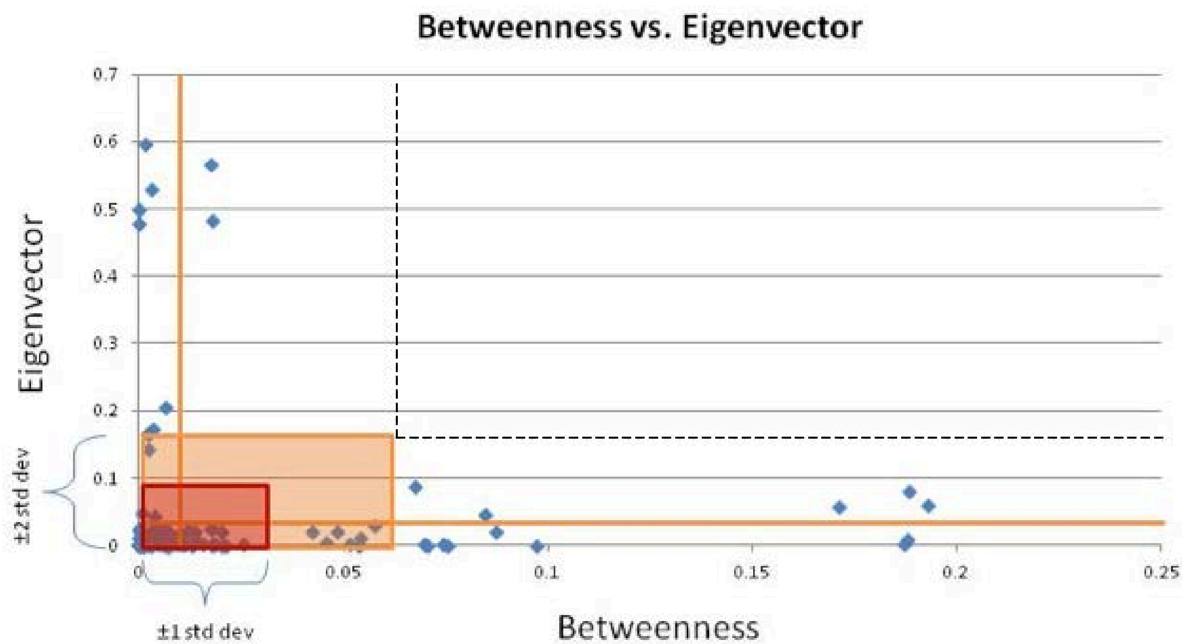
Analysis Techniques: Node Classification & Centrality Distribution

Node Classification: Technique #1

After analyzing the network for measures of centrality, the team developed a technique to ascertain node influence by integrating two measures into a single visualization.

Centrality measures can be related to actual distinctions of importance, which is very helpful when trying to parse data. Decision makers are often faced with trying to identify prominent individuals or organizations with influence over their neighbors or affiliates. Network analysis has the ability to mathematically determine these relationships. Our analysis incorporates the previously defined eigenvector centrality and betweenness centrality.

Graph 1 depicts the nodes in the network graphed by their values of the eigenvector and betweenness centralities. The colored boxes indicate the areas of the standard deviation from the mean of each particular centrality measure. Red is ±1 standard deviation and orange is ±2 standard deviations. The nodes outside of this range are those of interest and deserve a closer analysis. The asymptotes are located at the means of the centrality measure. The dotted lines divide the sections of the graph and allow us to designate roles to the actors in the regions.



Graph 1: Entity Network

The team has classified nodes that fall into the upper left quadrant (high in eigenvector centrality) as *Brokers*. Nodes in the lower right quadrant (high in betweenness centrality) were classified as *Gatekeepers.* The nodes in the upper right quadrant (both high in betweenness and eigenvector) were designated as *Superbrokers*. This combination of high values in both of the centrality measures would indicate some of the most influential agents or organizations in the network. Interestingly, this particular network contains no *Superbrokers*.

Node Classification: Technique #2

The usefulness of a classification method like the one described previously stems from its ability to help decision makers strategically identify who is actually influencing a network. Another proposed model of classification is the scoreboard approach illustrated in Table 3.

The scoreboard method of node classification is also based on each node's deviation from the mean in different network centrality measures. If the node is more than 1 standard deviation above the mean in value for a particular centrality measure then that node is labeled *High.* If a value was between +1 and -1 standard deviations then the node is labeled *Medium* and, if below or above 1 standard deviation it is labeled *Low*. The combination of these classifications across the selected measures gives us an indication of the role of any node in the network.

Node	**Betweenness**	**Closeness**	**Eigenvector**	**Degree**
Aerospace Industries Organization	High	High	Medium	High
Hafiz Darya Shipping Lines	Medium	Low	Medium	Medium
Neda Industrial Group	Medium	Low	High	High
Shiraz Electronics Industries	Medium	Medium	High	High
Reza Aghazadeh	High	Medium	Medium	Medium

Table 3: Example of classifications based on deviations from the mean of each centrality.

The nodes displayed in Table 3 were arbitrarily selected to illustrate this technique. The agents or organizations in the table represent the range of combinations of *High*, *Medium,* and *Low* rankings. The Aerospace Industries Organization appears to be very influential to the network based on its *High* rating in the three of the centrality measures and a *Medium* in the fourth. Likewise, the Hafiz Darya Shipping Lines is lower in most of the categories and might be given a classification such as *Peripheral Actor* in the network. Such a technique can quickly identify influential nodes in a complex network.

The team created an initial framework to assist in node classification and developed a scale of *Peripheral* to *Central*. Figure 4 illustrates the framework's scale and a potential node classification methodology. For example, if a node has 4 *High* values, 3 *High* values and 1 *Medium* value, or 3 High values and 1 *Low* value, it would be classified as *High Central*.

For a decision maker, being able to quickly generate a list of all of the influential nodes in the network could help cultivate a list of possible facilitators in the nuclear program development attempts in Iran. Using this scoreboard technique, the nodes can be analyzed quickly without having to use statistical methods which may prove to be more challenging and, perhaps, ineffective. A common statistical analysis of data would include counting modes, means and medians of data based on their appearances in the data set, then assigning an average number of appearances of how often an actor is listed as affiliated with another actor. This methodology does not quantify the influence of relationships in a data set like a network analysis technique.

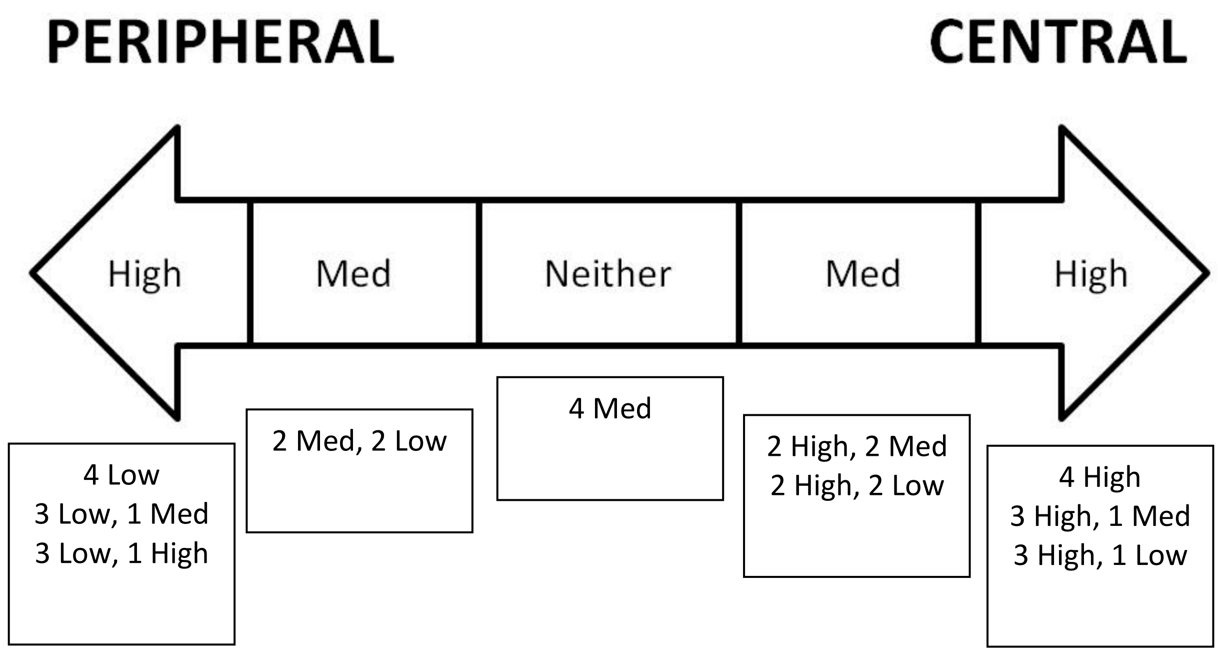


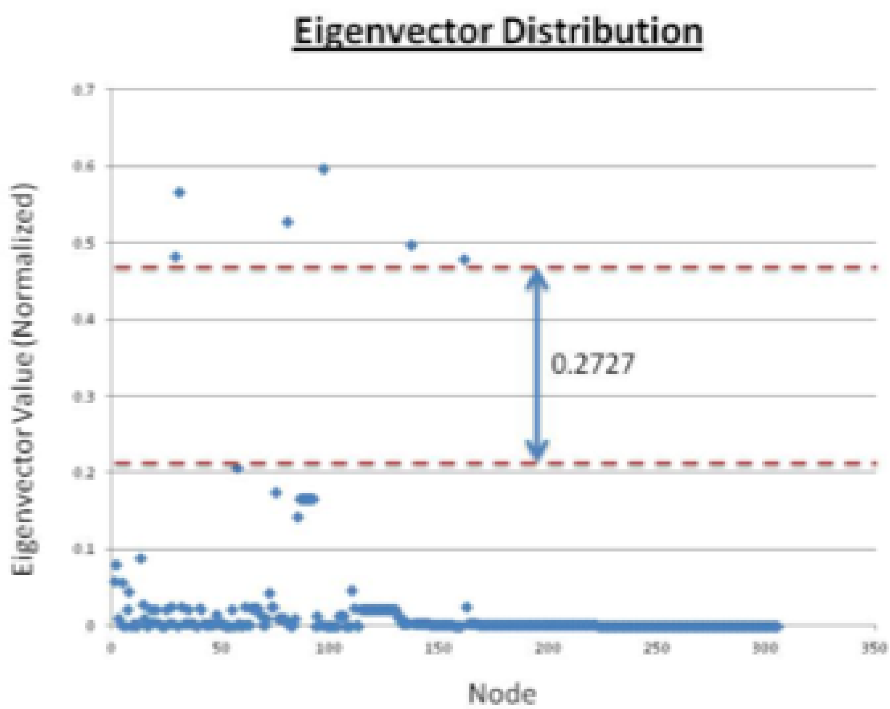
Figure 4: Scale of the classifications. Nodes move from peripheral levels to central levels. Below each classification are the ratings that fall in that level.

Additionally, this technique also assists in the classification of the overall network structure. The ability to classify a network structure equips policy makers with the ability to make inferences concerning the underlying relations within the network. Consequently, they now have the ability to effectively develop and execute strategic actions (sanctions for example) in order to disrupt the network, in this case, the efforts of Iran to develop nuclear weapons.

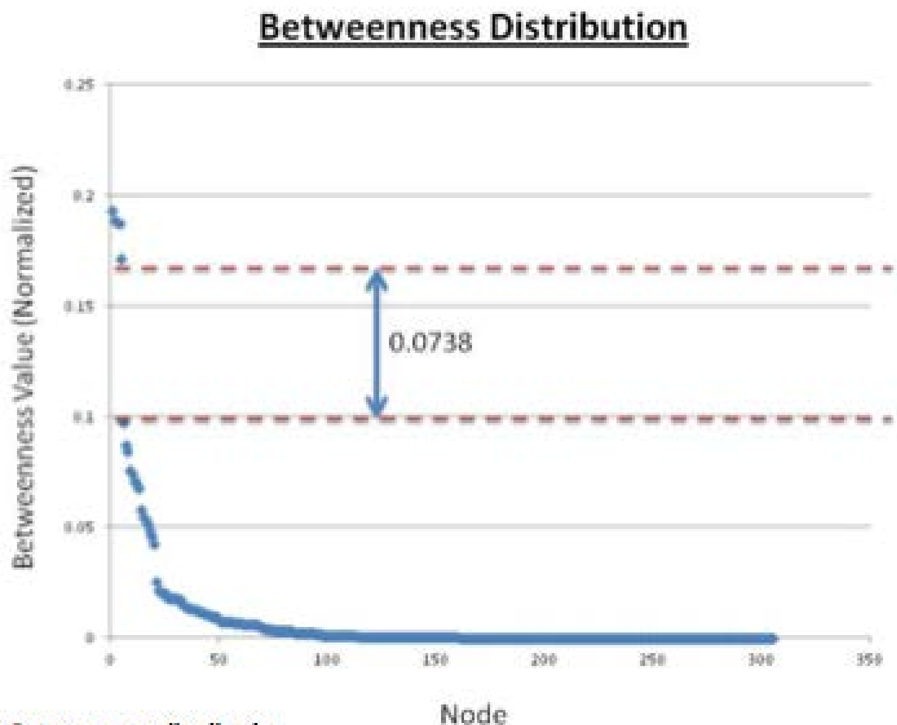
Centrality Distribution

The team then analyzed the distribution of the eigenvector and betweenness centrality measures of the nodes in the network in order to see if this provided additional insights on key agents and organizations in the network.

Graph 2 illustrates the distribution of eigenvector centrality in the Iran network. There is a noticeably large gap (.2727) between the nodes with high eigenvector centrality and those with low values. A major gap exists in the betweenness centrality (.0738) as well.



Graph 2: Eigenvector distribution reveals features of the structure of the network.



Graph 3: Betweenness distribution.

Visualizations such as these can be invaluable to a decision maker in determining the implementation of a sanction. Although this visualization highlights the same nodes that were identified in the previous technique, this technique more effectively illustrates the magnitude of influence when compared to the less influential nodes.

Conclusion and the Way Ahead

This paper has introduced several proposed methodologies for utilizing network analysis techniques in order to analyze a complex network like the Iranian nuclear development program. Analyzing nodes using multiple centrality measures and assigning roles to the nodes based on these metrics creates interesting analytical possibilities. This type of technique yields more information to a decision maker than simply analyzing individual nodes using one centrality measure. Once the nodes' roles are classified, decision makers have the capability to formulate an effective sanction plan.

In the future, the team proposes that this network be analyzed as it changes over time. For example, how did the network react or evolve to the imposition of a particular sanction? This behavior would yield great insights and additional characteristics that identify influential nodes. Additionally, the team proposes that techniques be developed that involve more than two centrality metrics and, perhaps, incorporate grouping algorithms in order to better understand sub-groups that exist in the network.

Finally, it should be noted, that the data collected for this project was from easily accessible, open-source information. Access to more accurate data would enable the development of a more precise model leading to specific effective recommendations.

References

[1] Kenneth Katzman, “Iran Sanctions,” Congressional Research Service, 16 July 2012. 30 July 2012 <http://www.fas.org/sgp/crs/mideast/RS20871.pdf>

[2] Al Arabiya, “Sanctions against Iran stymied efforts to produce ballistic missles: report,” Al Arabiya News, 30 July 2012. 30 July 2012 <http://english.alarabiya.net/articles/2012/07/30/229308.html>

[3] Emanuele Ottolenghi, “Are Iranian Sanctions Working?” Foundation for Defense of Democracies, 12 July 2012. 19 July 2012 <http://www.defenddemocracy.org/media-hit/are-iranian-sanctions-working/>

[4] David E. Thaler, Alireza Nader, Shahram Chubin, Jerrold D. Green, Charlotte Lynch and Frederic Wehrey, “Mullahs, Guards, and Bonyads: An Exploration of Iranian Leadership Dynamics,” RAND National Defense Research Institute, 2010. 19 July 2012.

[5] Kenneth Katzman, “Iran’s Bonyads: Economic Strengths and Weaknesses,” The Emirates Center for Strategic Studies and Research (ECSSR), 6 Aug 2006. 19 July 2012 <http://www.ecssr.com/ECSSR/appmanager/portal/ecssr?_nfpb=true&_nfls=false&_pageLabel=featuredTopicsPage&ftId=%2FFeatureTopic%2FKenneth_Katzman%2FFeatureTopic_0112.xml&lang=en&ftCountry=%2FCountries%2FCountry_0172.xml&_event=viewFeaturedTopic>

[6] Ulrik Brandes, Thomas Erlebach, “Network Analysis: Methodlogical Foundations,” Springer 2005. Pg. 20.

[7] Ulrik Brandes, Thomas Erlebach, “Network Analysis: Methodlogical Foundations,” Springer 2005. Pg. 29.

[8] Sabidussi, G. 1966. "The Centrality Index of a Graph." Psychometrika 31:581- 603.

[9] M. E. J. Newman, “The Mathematics of Networks.” (2008): Pennsylvania State University.

Appendix A

Betweenness Centrality Sized Entity Network

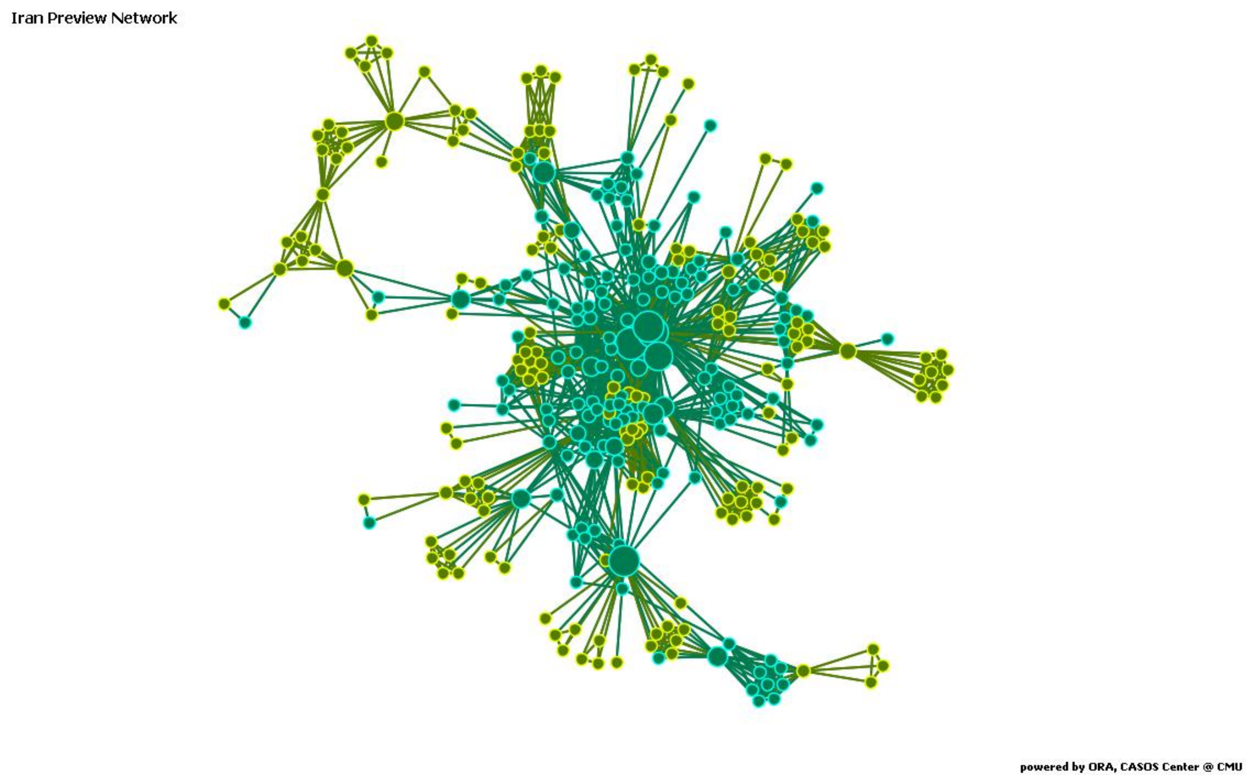


Figure above shows the single mode entity network. Entities have been colored by their descriptive attributes. Blue represents organizations and green represents individuals. Larger vertices are higher in betweenness centrality and those smaller are lower.

Appendix B

Closeness Centrality Sized Entity Network

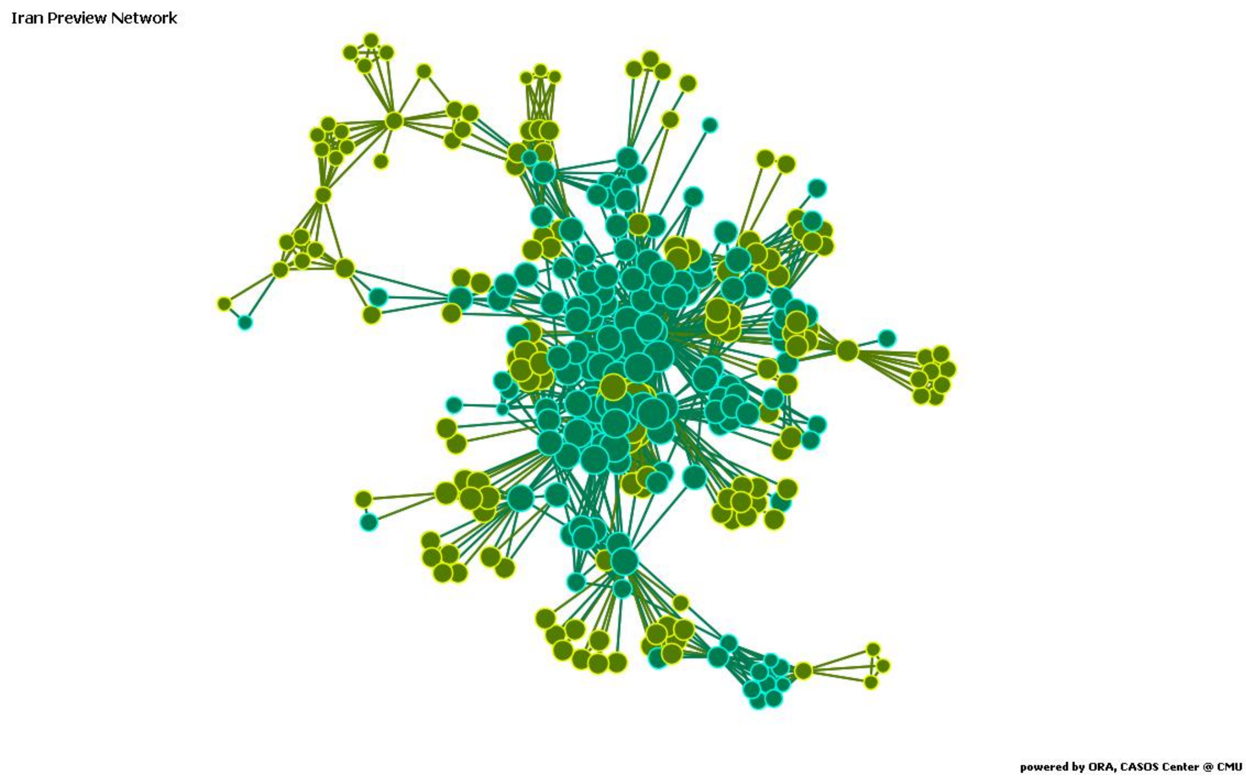


Figure above shows the single mode entity network. Entities have been colored by their descriptive attributes. Blue represents organizations and those that are green are individuals. Larger vertices are higher in closeness centrality and those smaller are lower. Notice the majority of vertices exhibit similar size in closeness centrality. This leads us to believe that there are many short paths in the network as well as vertices high in degree. This network should plausibly be able to transfer information, money, etc. fairly quickly.

Appendix C

Degree Centrality Sized Entity Network

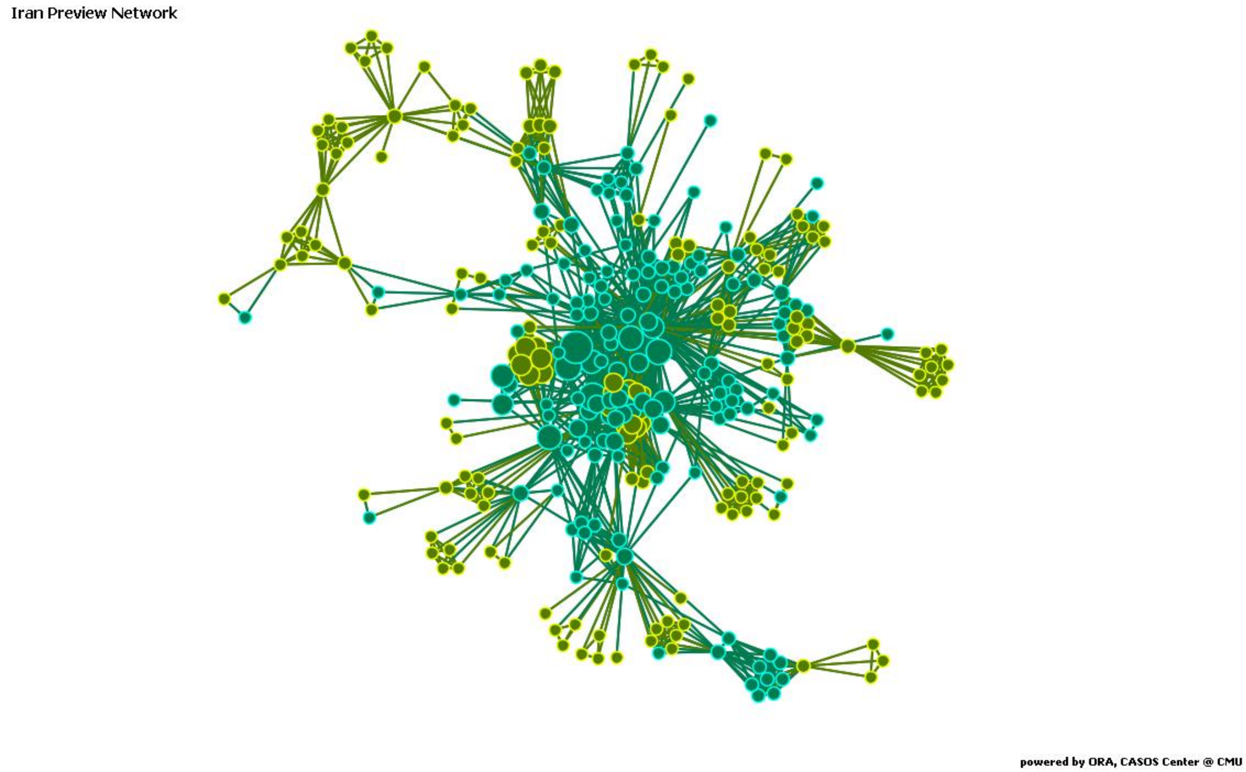


Figure above shows the single mode entity network. Entities have been colored by their descriptive attributes. Blue represents organizations and those that are green are individuals. Larger vertices are higher in degree centrality and those smaller are lower. The vertices high in degree are grouped together near the center of the graph leading us to believe that the network revolves around a core of closely connected organizations.

Appendix D

Eigenvector Centrality Sized Entity Network

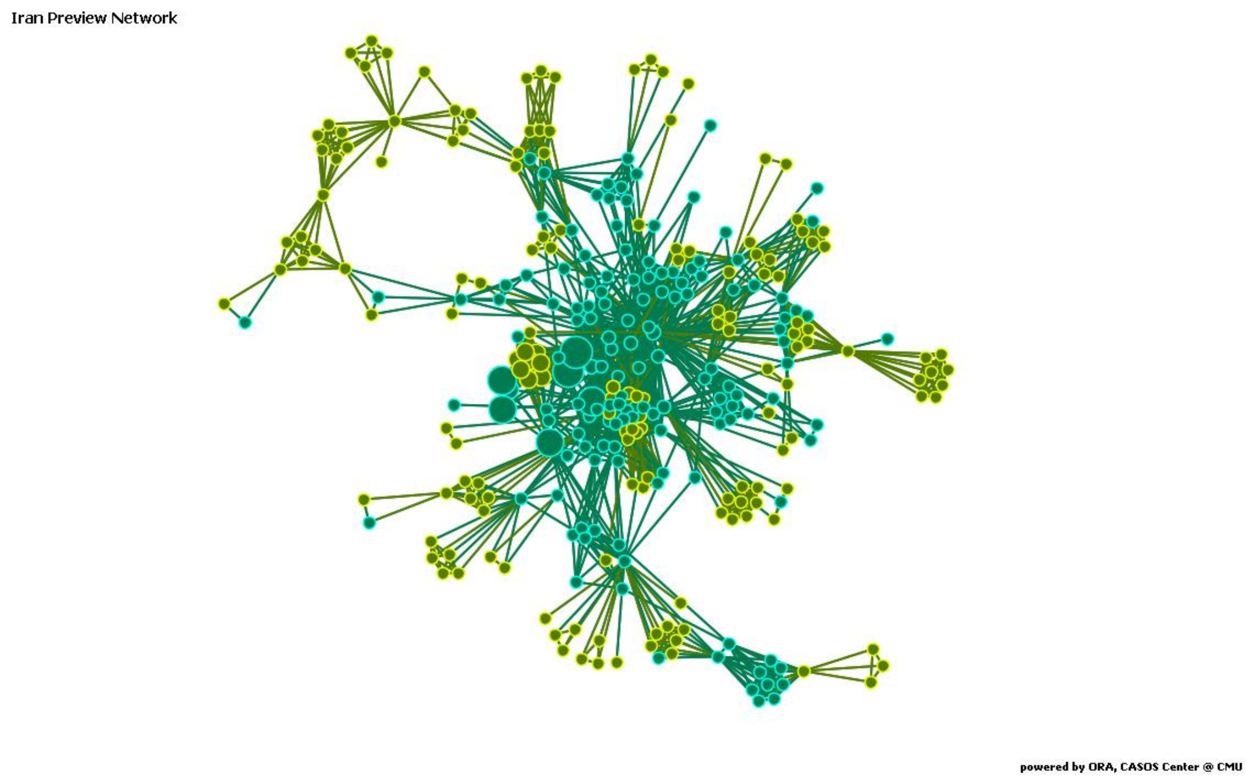


Figure above shows the single mode entity network. Entities have been colored by their descriptive attributes. Blue represents organizations and those that are green are individuals. Larger vertices are higher in eigenvector centrality and those smaller are lower.